Joe Bardwell
Vice President of Professional Services
WildPackets, Inc.

Introduction

Questions have arisen regarding the choices presented in the AiroPeek Options/Configuration pulldown menu under the 802.11 tab. This document describes their similarities and differences.

AiroPeek provides two fundamentally different 802.11 configuration options for capturing WLAN packets. You will find three radio buttons in the 802.11 window of the configuration options: Channel, BSSID, and ESSID. The "Channel" option (allowing you to select a channel number) works differently from the BSSID and ESSID choices (allowing you to specify a value for the Access Point WLAN ID). To understand the distinction between these two different AiroPeek behaviors requires a brief technical perspective.

802.11 Channels

In 802.11b the "channel" number does not refer to a discrete, single frequency band, as would be the case if we were discussing television or radio "channels." When your favorite television program is on channel 5 it means that a single, contiguous frequency range (assigned the number 5 by the FCC) is being used for the audio, video, and image control signals. This is called, in television, the "NTSC" standard (in the United States). When the IEEE 802.11 committee uses the term "channel" they have something slightly different to represent. In the 802.11 standard the method of sending data is called "spread spectrum." This means that the actual RF signal energy is NOT constrained within a single discrete range of frequency like an NTSC television channel would be. Rather, each "channel" in 802.11 refers to a group of smaller, individually discrete ranges of frequencies. A loose analogy would be to think about the teeth in a hair comb. If you number the teeth from left to right then you might say that television channel 5 is transmitted using teeth 28 through 32. In 802.11 you would then describe "channel 6" as using teeth 3 and 4, 7 and 8, 13 and 14, and 17 and 18. The transmission of 802.11 data "hops" around between these different frequency ranges. Using this analogy, you might say that 802.11 channel 7 uses teeth 5 and 6, 9 and 10, 15 and 16, and 19 and 20. You see, there is actually some overlap in the actual RF frequencies used in numerically different 802.11 channels.

When you configure an Access Point to transmit on "channel 6," it uses the hopping scheme that is specified for channel 6 by the 802.11 standard. This is where the essence of the difference between the two AiroPeek methods begins to take shape.

Channels and ID Values

An 802.11 client machine is configured with either a BSSID or ESSID value. The Basic ID is shorter than the Extended ID but they are both, simply, byte strings. The ID value is used by the NIC to determine which 802.11 packets belong to the WLAN in which the client is configured. In this way there can be multiple wireless broadcast domains present in the same atmospheric space. When a wireless NIC is operating, it listens to ALL channels and attempts to identify which channel is carrying the correct ID with the strongest signal. The card then self-configures to "hop" only on that channels specified range of frequencies.

When you select the AiroPeek radio button that specifies either a BSSID or ESSID, you are configuring the AiroPeek NIC to behave in this "normal" manner. You will only see packets that have the specified ID. The NIC will attempt to locate the "best" channel that is carrying the specified ID. In this case, when you examine packets in the summary or detail window, you will see the channel number that was selected by the NIC. It is possible, in a case where multiple Access Points with the same ID are configured on different channels, to see frames in the buffer with different channel numbers. The card is aware of the possibility that the station is physically moving away from one Access Point and getting closer to another. Hence, the channel selected by the NIC can change in real-time.

On the other hand, when you select the AiroPeek radio button that specifies a channel number, you are overriding the "normal" behavior of the NIC and forcing it to use the frequency hopping algorithm and frequencies associated only with the specified channel. If there are multiple access points configured with different ID's, but using the specified channel, then you will see packets in the AiroPeek summary or detail window that have different BSSIDs or ESSIDs. Every packet will have the specified channel number indicated, since you have told the NIC to only receive signals using that channel’s frequencies.

With regard to the fact that the 802.11 channel assignments actually use overlapping ranges of frequencies, you will often see an initially strange behavior in an environment where multiple access points are present. You may find that packets transmitted by an Access Point configured for one particular channel are actually visible when AiroPeek is configured to use a different channel. The "foreign" packets will have a significantly smaller RF signal strength than the "correct" packets. These "foreign" packets are seen because of the overlap in the signal ranges. In the same way that you can sometimes hear a citizens band radio "bleeding over" into your car radio, or you can tune your radio to a frequency where you hear two different stations at the same time, the 802.11 signal discrimination allows RF signals to slightly interfere with each other. (Suffice it to say, your PCMCIA RF receiver circuitry is not designed to communicate to the Voyager space probe in deep space!) For this reason, you may have AiroPeek configured for channel 6 (for example), but you will capture traffic from an Access Point that you know is configured to use channel 7. AiroPeek is going to mark these “foreign” frames as "Channel 6," NOT the "correct" Channel 7. Why? Because you have selected channel 6 and AiroPeek has configured the NIC to use the channel 6 frequency ranges, but there is some RF bleed-over that places the channel 7 signals somewhat into the range used by channel 6 and the packets are acquired.

Remember that the "channel" mode is NOT similar to the "normal" Client/Server behavior used by stations in the WLAN. This is a special forced-configuration mode available in AiroPeek. You can get an idea of the amount of "bleed over" when you know the channel number that is, in fact, configured at the Access Point. If you have an Access Point configured for channel 6 and you set AiroPeek to channel 7, then you will know whether any channel 6 traffic is bleeding over to channel 7. If it is, and if you are planning on implementing a second Access Point for a different WLAN, then you should not pick channel 7 for the new Access Point. You have determined that the channel 7 signal space is being bled into by the channel 6 Access Point.

Note: See the 802.11b spec section 18.4.6.7.2 for a good explanation of overlapping channels. The center frequencies of each named channel are separated by 5MHz, but the signals are spread +/- 10 MHz from the center frequency, so there is intentional overlap with neighboring channels. Note that even in ESSID mode, traffic from other channels will be observed.

WildPackets Professional Services

WildPackets offers a full spectrum of unique professional support services, available on-site, online or through remote dial-in service.

On-Site Consulting

When protocol analysis support is needed at your site, the network experts at WildPackets will work with you and your support team to resolve network problems.

Performance Baseline and Network Capacity Planning Report

When it is necessary to know the real performance and capacity issues facing your network, a WildPackets consultant can create a baseline report, from a simple evaluation of a single critical server or router up to an assessment of your overall network infrastructure.

Infrastructure Design Analysis Services

The network experts at WildPackets can help you sort through the details of multi-vendor proposals for hardware and software installation and systems integration, providing you with an un-biased, third party perspective on your proposed network planning,

Remote Consulting Services

WildPackets' Remote Consulting Services may resolve challenging network problems for you without requiring an on-site visit. Our protocol analysis experts will accurately analyze specific trace files you send in to them or capture live traffic from your network and provide a general characterization of network performance and potential problems.

WildPackets Academy

WildPackets Academy offers the most effective and comprehensive network and protocol analysis training available, meeting the professional development and training requirements of corporate, educational, government, and private network managers. Our instructional methodology and course design centers around practical applications of protocol analysis techniques for both Ethernet and 802.11b wireless LANs. WildPackets Academy also provides instruction and testing for the industry-standard **NAX™ (Network Analysis Expert) Certification.**

For more information about consulting and educational services, including complete course catalog, pricing and scheduling, please visit http://www.wildpacketsacademy.com. NAX examination and certification details are available at http://www.nax2000.com.

Live Online Quick Start Program

WildPackets now offers one-hour online Quick Start Programs on using EtherPeek and AiroPeek, led by a WildPackets Academy Instructor. Please visit http://www.wildpackets.com/events for complete details and scheduling information.

WildPackets, Inc.

Since its inception in 1990, WildPackets has been developing affordable tools designed to simplify the complex tasks associated with designing, maintaining, troubleshooting and optimizing computer networks. In the past eighteen months, WildPackets has acquired two key partner organizations and greatly expanded its product development expertise and professional services capabilities in the process. WildPackets customers include Ameritech, Cisco Systems, Lucent Technologies, Microsoft, National Institutes of Health, Yahoo! and others. Strategic partners include Cisco Systems, Symbol Technologies and Agere Systems.

WildPackets, Inc.
2540 Camino Diablo
Walnut Creek, CA 94596
Tel 925-937-7900
Fax 925-937-2479
www.wildpackets.com